Copyright 2013 ValuePoint Networks, Inc. All rights reserved.

Hotel Brand Standards Guide

VP Networks gateways meet all major hotel brand standards. This guide provides guidance for some of the brands. It is merely a partial list, please consult with your VP Networks representative if you have any questions, or for guidance on any brand not on this list.

All trademarks and logos in the document are the property of their respective owners.

December 2012

Copyright 2013 ValuePoint Networks, Inc. All rights reserved.

Table of Contents

1. Best Western 3
    1.1. Overview 3
    1.2. Gateway Configuration: 3
    1.3. Other Requirements 4
2. Choice Hotels 5
    2.1. Overview 5
    2.2. Gateway Configuration: 5
    2.3. Access Point Configuration 6
    2.4. Other Requirements 6
3. IHG (includes Holiday Inn) 7
    3.1. Overview 7
    3.2. Gateway Configuration: 7
    3.3. Access Point Configuration 9
    3.4. Other Requirements 9
4. Hampton Inn 10
    4.1. Overview 10
    4.2. Gateway Configuration: 10
    4.3. Access Point Configuration 12
    4.4. Other Requirements 12
5. Marriott/Select Brand 13
    5.1. Overview 13
    5.2. Gateway Configuration: 13
    5.3. Access Point Configuration 15
    5.4. Other Requirements 15
6. Ramada Inn 16
    6.1. Overview 16
    6.2. Gateway Configuration: 16
    6.3. Access Point Configuration 18
    6.4. Other Requirements 18
7. Starwood 19

Copyright 2013 ValuePoint Networks, Inc. All rights reserved.

1. Best Western

1.1. Overview

ValuePoint Networks is on the approved hardware vendor list from Best Western™.

1.2. Gateway Configuration:

1.2.1. Auto-IP

Customers with static IP configuration must be able to access the internet. Enable Auto-IP in the Controller under **Networks – System – Auto-IP.**

1.2.2. DHCP Server

DHCP is enabled by default. Configure according to your design under **Networks – Server – DHCP Server**.

1.2.3. Auto Proxy

Best Western requires customers configured to a common HTTP Proxy address to be able to browse web pages. Enable Auto-Proxy under **Networks – System – Server – Auto-Proxy**.

1.2.4. VPN Static IPs

You must provide additional routable static IP addresses for customers to establish VPN connections. You or the hotel must purchase additional static IP addresses from the ISP. Enable this feature under **Advanced – VPN Static IPs**. Please see the product manual for full details on configuring this feature.

1.2.5. Client Isolation

Best Western requires that guests not be able to ping or access each others computer's on the network. This can be done in two ways:

1. Controller Subscriber VLAN: Enable Subscriber VLAN in the Controller under Networks – System – Subscriber VLAN. In this configuration the Controller will block any customer – customer traffic that it sees. However, the Controller may not ever see this traffic on a switched LAN network or if two customers are on the same Access Point.

Copyright 2013 ValuePoint Networks, Inc. All rights reserved.

It should also be noted that a single ping may succeed between customers before the Controller configures the Subscriber VLAN.

2. Access Point Subscriber VLAN: In order to block traffic on the other side of a switch from the Controller, or on the same AP, it may be necessary to enable client isolation on each Access Point. The ValuePoint SuperAP includes this feature.

A combination of #1 and #2 gives the best customer security.

1.3. Other Requirements

- UPS capable of powering the whole network from a battery for 20 minutes.
- Must provide Guest Access Hardware. This can be PCMCIA lender cards or a wireless bridge device.
- VLAN on the public network. This will require VLAN enabled hardware at all points including switches and APs.
- Network must cover 15% of rooms, either wired or wirelessly
- Must provide in room literature
- Minimum ISP connection speed of 512Kbps.
- 1-800 or local support number with 24/7 access.

Copyright 2013 ValuePoint Networks, Inc. All rights reserved.

2. Choice Hotels

2.1. Overview

VP Networks products are used in thousands of Choice Hotels properties world-wide, and meet all requirements.

2.2. Gateway Configuration:

2.2.1. Terms of Service Page

Choice requires that the customer accept terms of service before accessing the HSIA. You can enforce acceptance of these terms using a terms of service page hosted either internally using the built-in terms of service page, or hosted externally.

2.2.2. Post-Authentication Redirect

Choice requires that customers be directed to a property specific web page after the customers accepts the terms of service. There is a standardized location (URL) to send customers to. Enter this URL under **Customization – Login Page – Post-Authentication Redirect – Specify URL**. This URL may take the form of:

http://www.choicehotels.com/hotel/<property_code>

You must get this property code from Choice or the hotel owner. Choice may provide a page template at

http://www.choicebuys.com/hsia

2.2.3. Auto-IP

Customers with static IP configuration must be able to access the internet. Enable Auto-IP in the Controller under **Networks – System – Auto-IP.**

2.2.4. Auto Proxy

Choice requires “Plug and Play” for customers, so probably Auto-Proxy is required. Customers configured to a common HTTP Proxy address will able to browse web pages. Enable Auto-Proxy under **Networks – System – Server – Auto-Proxy**.

Copyright 2013 ValuePoint Networks, Inc. All rights reserved.

2.2.5. VPN Static IPs

You must provide additional routable static IP addresses for customers to establish VPN connections. You or the hotel must purchase additional static IP addresses from the ISP. Enable this feature under Advanced – VPN Static IPs. Please see the product manual for full details on configuring this feature. ValuePoint does not have information on how many static IP addresses are required for customers use. 5 to 10 is typical in other deployments.

2.2.6. Remote access to network hardware

After installation the Controller can be accessed by directing your browser to the Static IP address. You can also access the web interfaces of other hardware in the system by adding individual devices to the AP Monitor. You can configure this under **Management – Access Point Monitor**. During operation you can monitor and access APs under **Status – APs**.

2.3. Access Point Configuration

2.3.1. Minimum 1Mbps connection speed at each covered room

Choice does not specify what kind of hardware will be used to measure this.

2.4. Other Requirements

- Must provide Guest Access Hardware including cat5 Ethernet cables and **Wireless Bridge** devices. There should be both cat5 cables and Wireless Bridge devices equal to 10% of the rooms.
- Must cover all public spaces of hotel, dining, meeting rooms, etc.
- Minimum ISP connection speed of 512Kbps. ISP account must be Business DSL, Business Cable, or full/fractional T1.
- 1-800 support number required with 24x7 access.

Copyright 2013 ValuePoint Networks, Inc. All rights reserved.

3. IHG (includes Holiday Inn)

3.1. Overview

IHG includes the Holiday Inn™ brand. VP Networks products are used in thousands of IHG properties world-wide and are highly recommended by IHG's corporate technology team.

3.2. Gateway Configuration:

3.2.1. Login Page

Holiday Inn requires that customers login using a passcode that is changed on a weekly basis. The guest must also accept the terms of service before accessing the HSIA. You can enforce acceptance of these terms and the passcode using a custom portal page hosted either internally (Internal_portal.htm), or hosted externally. We have a number of sample pages we provide to customers to help get started with the IHG page.

3.2.2. Post-Authentication Redirect

Holiday Inn requires that customers be directed to a site specific web page after the customers accepts the terms of service. You must provide the location (URL) to send customers to. Enter this URL under **Customization – Login Page – Post-Authentication Redirect – Specify URL**. You must get this URL from Holiday Inn or the hotel owner, or create and host a page.

3.2.3. Auto-IP

Customers with static IP configuration must be able to access the internet. Enable Auto-IP in the Controller under **Networks – System – Auto-IP.**

3.2.4. DHCP Server

DHCP is enabled by default. Configure according to your design under **Networks – Server – DHCP Server**. The DHCP Pool should be 130% of the number of rooms.

3.2.5. Auto Proxy

Holiday Inn requires "Plug and Play" for customers, so probably Auto-Proxy is required. Customers configured to a common HTTP Proxy address will able to browse web pages. Enable Auto-Proxy under **Networks – System – Server – Auto-Proxy**.

Copyright 2013 ValuePoint Networks, Inc. All rights reserved.

3.2.6. VPN Static IPs

You must provide additional routable static IP addresses for customers to establish VPN connections. You or the hotel must purchase additional static IP addresses from the ISP. Enable this feature under Advanced – VPN Static IPs. Please see the product manual for full details on configuring this feature.

3.2.7. Client Isolation

Holiday Inn requires that guests not be able to ping or access each others computer's on the network. This can be done in two ways:

1. Controller Subscriber VLAN: Enable Subscriber VLAN in the Controller under Networks – System – Subscriber VLAN. In this configuration the Controller will block any customer – customer traffic that it sees. However, the Controller may not ever see this traffic on a switched LAN network or if two customers are on the same Access Point. It should also be noted that a single ping may succeed between customers before the Controller configures the Subscriber VLAN.

2. Access Point Subscriber VLAN: In order to block traffic on the other side of a switch from the Controller, or on the same AP, it may be necessary to enable client isolation on each Access Point. The ValuePoint SuperAP includes this feature.

A combination of #1 and #2 gives the best customer security.

3.2.8. SSL encrypted Management GUI

The management interface of network hardware must by protected by HTTPS privacy using SSL. The can be configured under **Networks – Server – Web Server – HTTPS**. Note that SSL will cause management pages to load more slowly due to the encryption.

3.2.9. Usage Throttling

In order to prevent one customer from monopolizing the network, Holiday Inn requires a limit on each customer's total bandwidth. Configure this on the Controller 3500 under **Networks – WAN/LAN – Subscriber Bandwidth Limitation**. This feature is not available on the Controller 3000. Contact Holiday Inn for more information on what the exact limit should be (128kbps, etc.)

3.2.10. Walled Garden

Holiday Inn specifies that they want a Walled Garden that allows access to hotel amenities without the customer having to log in to the system. Contact the site owner for more details on what they want in the walled garden.

3.2.11. Public and Meeting Room Log In

Connections in meetings rooms and public spaces must provide a log in page rather

Copyright 2013 ValuePoint Networks, Inc. All rights reserved.

than the terms of service of service page in guest rooms.

3.3. Access Point Configuration

3.3.1. SSL Encrypted Management GUI

The management interface for the AP must be SSL (https://) encrypted. This functionality is supported in the SuperAP 570n from ValuePoint. Otherwise consult your AP documentation.

3.3.2. Minimum connection speeds

Holiday in requires 1Mbps in guest rooms and 200Kbps in public spaces. Holiday Inn does not specify what kind of hardware will be used to measure this.

3.4. Other Requirements

- Must cover all guest rooms, public spaces, dining and meeting rooms wirelessly. At least one meeting room must have a wired connection.
- Must provide Guest Access Hardware for wireless only installations. The Holiday Inn specification mentions a **Wireless Bridge** device, which is probably a AC or USB powered Wireless Client with an Ethernet port on it. The Wireless Bridge must be preconfigured for WEP 128. There should be Wireless Bridge devices equal to 10% of the rooms.
- VLAN on the public network. This will require VLAN enabled hardware at all points including switches and APs.
- Must provide in room literature
- Must separate public network from hotel administration network.
- SPAM Control: Holiday Inn specifies that they want outbound SPAM control, but gives no details.
- Minimum ISP connection speed of 1.5Mbps.
- Troubleshooting and support for guests required, but not specified in terms of toll free, hours, etc.
- ”Network Intrusion Detection”. Holiday Inn does not define what they mean by this, so it is not clear how this would be accomplished. Contact Holiday Inn for more information.

3.4.1. SMTP Email Issues

Holiday Inn specifies SMTP email support as part of the certification. SMTP mail will be delivered by default to its configured destination (SMTP.mail.com, etc.) You can configure the Controller to intercept outgoing SMTP and redirect it to a SMTP server that

Copyright 2013 ValuePoint Networks, Inc. All rights reserved.

you specify. In this case **your SMTP server** is responsible for delivering these messages, some of which may be encrypted and some not. The Controller does not modify these messages in any way, it just redirects them to your SMTP server. If you want to redirect SMTP email you can configure this under **Networks – System – Server – SMTP Redirect.**

4. Hampton Inn

4.1. Overview

Hampton Inn™ is a HiltonFamily™ brand, but includes requirements for authentication against a proprietary High Speed Internet Access (HSIA) service centrally provided by Hampton Inn. Other HiltonFamily properties may be using this system. Contact Hilton for more information.

You must be 80% compliant with the Hampton Inn requirements to pass their certification test. We do not have any details on cost or how to arrange the certification test at the hotel site.

4.2. Gateway Configuration:

4.2.1. Hampton Inn HSIA Authentication

You must configure the Controller to use Hampton Inn's proprietary authentication mechanism. Enable Hampton Inn HSIA under **Security – Authentication – Hampton Inn**.

You must configure the Hampton HSIA Authentication with the correct values obtained from Hampton Inn or the property owner.

Central Authentication Server: The Hampton Server may be located at:

http://hsia.hamptoninn.com/hsia/servlet/AuthenticationRequest

However, there is no guarantee that this will be the correct server address for your site. You must make certain you have the correct server address from Hampton Inn or the property owner.

Property Code: Hampton Inn assigns a code to each property. ValuePoint does not have and can't get this code.

Property Zip: Mailing address Zip code

Gateway IP: This value is not necessary unless the Controller does not have a public

Copyright 2013 ValuePoint Networks, Inc. All rights reserved.

static IP address. This is not typical, but see the documentation if you need this feature.

Hampton Inn HSIA Authentication consists primarily of a “password of the week” for each Hotel. For testing purposes you must get a valid password from Hampton Inn or the property owner that matches the Property Code and Property Zip.

4.2.2. Auto-IP

Customers with static IP configuration must be able to access the internet. Enable Auto-IP in the Controller under **Networks – System – Auto-IP.**

4.2.3. DHCP Server

DHCP is enabled by default. Configure according to your design under **Networks – Server – DHCP Server**.

4.2.4. Auto Proxy

Hampton Inn requires customers configured to a common HTTP Proxy address to be able to browse web pages. Enable Auto-Proxy under **Networks – System – Server – Auto-Proxy**. The default values are common proxy servers, including 8080 which Hampton specifically tests in their site review. Consult the latest Hampton Inn requirements for additional ports they may test.

4.2.5. VPN Static IPs

You must provide additional routable static IP addresses for customers to establish VPN connections. You or the hotel must purchase additional static IP addresses from the ISP. Enable this feature under Advanced – VPN Static IPs. Please see the product manual for full details on configuring this feature. ValuePoint does not have information on how many static IP addresses are required for customers use. 5 to 10 is typical in other deployments.

4.2.6. Client Isolation

Hampton Inn requires that guests not be able to ping or access each others computer’s on the network. This can be done in two ways:

1. Controller Subscriber VLAN: Enable Subscriber VLAN in the Controller under Networks – System – Subscriber VLAN. In this configuration the Controller will block any customer – customer traffic that it sees. However, the Controller may not ever see this traffic on a switched LAN network or if two customers are on the same Access Point. It should also be noted that a single ping may succeed between customers before the Controller configures the Subscriber VLAN.

2. Access Point Subscriber VLAN: In order to block traffic on the other side of a switch from the Controller, or on the same AP, it may be necessary to enable client isolation on each Access Point. The ValuePoint SuperAP includes this feature.

A combination of #1 and #2 gives the best customer security.

Copyright 2013 ValuePoint Networks, Inc. All rights reserved.

4.3. Access Point Configuration

4.3.1. Minimum 5.5Mbps connection speed across entire hotel

Hampton does not specify what kind of hardware will be used to measure this beyond a laptop with NetStumbler.

4.3.2. No overlapping AP Channels

Hampton does a test to look for overlapping APs on the same channel. Use best practices for AP coverage, or use 4 channels instead of three. Hampton does not specify what kind of hardware will be used to measure this beyond a laptop with NetStumbler.

4.3.3. SSID=HHONORS

This requirement also covers the WC-3000 (with built in AP) if you are using a public SSID in that device. **Configure SSID under Networks – Wireless – SSID**.

4.4. Other Requirements

- Hampton Inn Certification of site required
- Must cover all public spaces of hotel, dining rooms, meeting rooms, etc.
- Must provide Guest Access Hardware. Presumably this means NIC cards, cat5 cables, or a stand alone wireless client device.
- Must provide in room literature
- Must separate public network from hotel administration network.
- SPAM Control: In your ISP or NOC SMTP server you must limit outgoing messages to 100 recipient addresses and filter for common SPAM words. ValuePoint does not have any information on what Hampton Inn's definition of "common spam words" is. This functionality must be implemented in your SMTP server. The Controller cannot filter e-mail.
- Minimum www.dslreports.com speed test result of 435Kbps up to 150 rooms, 1275Kbps more than 150 rooms.
- 1-800 support number required with live representative

4.4.1. SMTP Email Issues

There is an SMTP email test as part of the certification, but ValuePoint does not have

Copyright 2013 ValuePoint Networks, Inc. All rights reserved.

details on the nature of this test. SMTP mail will be delivered by default to its configured destination (smtp.mail.com, etc.) You can configure the Controller to intercept outgoing SMTP and redirect it to a SMTP server that you specify. In this case **your SMTP server** is responsible for delivering these messages, some of which may be encrypted and some not. The Controller does not modify these messages in any way; it just redirects them to your SMTP server. If you want to redirect SMTP email you can configure this under **Networks – System – Server – SMTP Redirect.**

5. Marriott/Select Brand

5.1. Overview

You must be compliant with the Marriott™ requirements to pass their certification test. The section below covers 'required' elements. There are other 'recommended' elements as well that the property owner may want.

5.2. Gateway Configuration:

5.2.1. Terms of Service Page

Marriott requires that the customer accept the terms of service before accessing the HSIA. You can enforce acceptance of these terms using a terms of service page.

An externally hosted terms of service page requires that you have a HTTP server in your NOC, or a hosted page somewhere else. There is sample code you can use on your terms of service page under **Maintenance – System Tools – Terms of Service – View External HTML Code**. You must put this post form on your HTML page and not change the values of the <form> or <input> HTML tags.

5.2.2. Post-Authentication Redirect

Marriott requires that customers be directed to a property specific web page after the customers accepts the terms of service. There is a standardized location (URL) to send customers to. Enter this URL under **Customization – Login Page – Post-Authentication Redirect – Specify URL**. This URL may take the form of:

http://<brandsite.com>/<property_code>

You must get this property code (MARSHA?) from Marriott or the hotel owner.

5.2.3. Auto-IP

Customers with static IP configuration must be able to access the internet. Enable Auto-IP in the Controller under **Networks – System – Auto-IP.**

Copyright 2013 ValuePoint Networks, Inc. All rights reserved.

5.2.4. DHCP Server

DHCP is enabled by default. Configure according to your design under **Networks – Server – DHCP Server**.

5.2.5. VPN Static IPs

You must provide additional routable static IP addresses for customers to establish VPN connections. You or the hotel must purchase additional static IP addresses from the ISP. Enable this feature under Advanced – VPN Static IPs. Please see the product manual for full details on configuring this feature. ValuePoint does not have information on how many static IP addresses are required for customer use at a particular hotel. 10 is currently the maximum in the Controller 3000, 200 for the Controller 3500.

5.2.6. Remote access to network hardware

After installation the Controller can be accessed by directing your browser to the Static IP address. You can also access the web interfaces of other hardware in the system by adding individual devices to the AP Monitor. You can configure this under **Management – Access Point Monitor**. During operation you can monitor and access APs under **Status – APs**.

5.2.7. PMS Interface

HSIA access that is billed to the room must support the appropriate PMS interface for the hotel in question. This could be one of Micros Fidelio, Courtyard PMS, Richie PMS, MHRS Full Service PMS, and Pegasus Guestview. The Controller 3000 does not support PMS, so you will need to use the Controller 3500.

5.2.8. Configuration Backup

The Controller Configuration can be backed and restored under **System Tools – Maintenance – Configuration**.

5.2.9. SSL encrypted Authentication

Authentication must by protected by HTTPS privacy using SSL. The can be configured under **Networks – Server – Web Server – HTTPS**. Note that this will SSL encrypt the Controller GUI as well, which will cause management pages to load more slowly due to the encryption.

5.2.10. Client Isolation

Marriot requires that guests not be able to ping or access each others computer's on the network. This can be done in two ways:

1. Controller Subscriber VLAN: Enable Subscriber VLAN in the Controller under Networks – System – Subscriber VLAN. In this configuration the Controller will block

Copyright 2013 ValuePoint Networks, Inc. All rights reserved.

any customer – customer traffic that it sees. However, the Controller may not ever see this traffic on a switched LAN network or if two customers are on the same Access Point. It should also be noted that a single ping may succeed between customers before the Controller configures the Subscriber VLAN.

2. Access Point Subscriber VLAN: In order to block traffic on the other side of a switch from the Controller, or on the same AP, it may be necessary to enable client isolation on each Access Point. The ValuePoint SuperAP includes this feature.

A combination of #1 and #2 gives the best customer security.

5.3. Access Point Configuration

5.3.1. Minimum 1Mbps connection speed at each covered room

Marriot does not specify what kind of hardware will be used to measure this. Marriott reports that they would prefer 5.5Mbps

5.4. Other Requirements

- Certification by Marriot required
- Must provide in room literature.
- Must separate public network from hotel administration network.
- Minimum 512Kbps connection to ISP.
- 1-800 support number required
- Insurance coverage of some kind is required. ValuePoint does not have details on what Marriott requires.
- Routable Static IP Address required for each customer. For 100 simultaneous users this would require a block of 100 static IP addresses. This would be something to clarify with Marriott.

5.4.1. SMTP Email Issues

There is an SMTP email test as part of the certification, but ValuePoint does not have details on the nature of this test. SMTP mail will be delivered by default to its configured destination (SMTP.mail.com, etc.) You can configure the Controller to intercept outgoing SMTP and redirect it to a SMTP server that you specify. In this case **your SMTP server** is responsible for delivering these messages, some of which may be encrypted and some not. The Controller does not modify these messages in any way; it just redirects them to your SMTP server. If you want to redirect SMTP email you can configure this under **Networks – System – Server – SMTP Redirect.**

Copyright 2013 ValuePoint Networks, Inc. All rights reserved.

6. Ramada Inn

6.1. Overview

Ramada Inn™ seems to allow self-certification to their standard. Contact Ramada for full details. Ramada is a member of the Cendant Hotel brand, but it is not known if other Cendant hotels have the same requirements. Contact Cendant or the site owner for more information.

There appear to be two Ramada/Cendant standards. The requirements we give below are based on what Ramada provided in August 2005. Ramada may have additional requirements for "larger" (150+ rooms) sites similar to the Hilton requirements with regard to Multi-SSID APs and Public VLAN. It is recommended that you make certain that you have the correct and current requirements for your site from Ramada or the site owner directly before doing the installation.

6.2. Gateway Configuration:

6.2.1. Terms of Service Page

Ramada requires that the customer accept the terms of service before accessing the HSIA. You can enforce acceptance of these terms using a terms of service page.

An externally hosted terms of service page requires that you have a HTTP server in your NOC, or a hosted page somewhere else. There is sample code you can use on your terms of service page under **Maintenance – System Tools – Terms of Service – View External HTML Code**. You must put this post form on your HTML page and not change the values of the <form> or <input> HTML tags.

6.2.2. Post-Authentication Redirect

Ramada requires that customers be directed to a Ramada branded or site specific web page after the customers accepts the terms of service. You must provide the location (URL) to send customers to. Enter this URL under **Customization – Login Page – Post-Authentication Redirect – Specify URL**. You must get this URL from Ramada or the hotel owner, or create and host a page acceptable to Ramada. There is some suggestion that just www.ramada.com would be acceptable.

6.2.3. Auto-IP

Customers with static IP configuration must be able to access the internet. Enable Auto-IP in the Controller under **Networks – System – Auto-IP.**

Copyright 2013 ValuePoint Networks, Inc. All rights reserved.

6.2.4. Auto Proxy

Ramada requires “Plug and Play” for customers, so probably Auto-Proxy is required. Customers configured to a common HTTP Proxy address will able to browse web pages. Enable Auto-Proxy under **Networks – System – Server – Auto-Proxy**.

6.2.5. DHCP Server

DHCP is enabled by default. Configure according to your design under **Networks – Server – DHCP Server**.

6.2.6. VPN Static IPs

You must provide additional routable static IP addresses for customers to establish VPN connections. You or the hotel must purchase additional static IP addresses from the ISP. Enable this feature under Advanced – VPN Static IPs. Please see the product manual for full details on configuring this feature. ValuePoint does not have information on how many static IP addresses are required for customers use. 5 to 10 is typical in other deployments.

6.2.7. Client Isolation

Ramada requires that guests not be able to ping or access each others computer’s on the network. This can be done in two ways:

1. Controller Subscriber VLAN: Enable Subscriber VLAN in the Controller under Networks – System – Subscriber VLAN. In this configuration the Controller will block any customer – customer traffic that it sees. However, the Controller may not ever see this traffic on a switched LAN network or if two customers are on the same Access Point. It should also be noted that a single ping may succeed between customers before the Controller configures the Subscriber VLAN.

2. Access Point Subscriber VLAN: In order to block traffic on the other side of a switch from the Controller, or on the same AP, it may be necessary to enable client isolation on each Access Point. The ValuePoint SuperAP includes this feature.

A combination of #1 and #2 gives the best customer security.

6.2.8. Usage Throttling

In order to prevent one customer from monopolizing the network Ramada requires a limit on each customer’s total bandwidth. Configure this on the Controller 3500 under **Networks – WAN/LAN – Subscriber Bandwidth Limitation**. This feature is not available on the Controller 3000. Contact Ramada for more information on what the exact limit should be (128kbps, etc.)

6.2.9. Local Hardware Management by Hotel Personnel

Ramada requires the on site staff be able to monitor user activity, terminate users, and create access accounts. You can create a **Subscriber Manager** account to do this that

Copyright 2013 ValuePoint Networks, Inc. All rights reserved.

does not have access to the network configuration. Configure the username/password under **System Tools – Admin – Subscriber Manager**.

6.3. Access Point Configuration

6.3.1. Power over Ethernet

Ramada requires that Access Points be powered by Power over Ethernet. All ValuePoint APs support IEEE 802.3af standard PoE.

6.3.2. 802.11.b and .g support

Ramada requires that Access Points support both 802.11b and 802.11g.

6.3.3. No WEP or Authentication on APs

Access Point privacy using WEP, WPA, AES or others should be disabled.

6.3.4. Common SSID

All APs should use the same SSID for customer access.

6.4. Other Requirements

- One wired connection available in Public Area.
- Must cover all public spaces of hotel, dining, meeting rooms, etc.
- Must provide in room literature
- Must separate public network from hotel administration network.
- Minimum ISP connection speed of 512Kbps up to 150 rooms, 1.5Mbps more than 150 rooms.
- 1-800 support number required with 24x7 access.

6.4.1. SMTP Email Issues

There is an SMTP email support requirement by Ramada, but ValuePoint does not have details on how or what they plan to test. SMTP mail will be delivered by default to its configured destination (SMTP.mail.com, etc.) You can configure the Controller to intercept outgoing SMTP and redirect it to a SMTP server that you specify. In this case **your SMTP server** is responsible for delivering these messages, some of which may be encrypted and some not. The Controller does not modify these messages in any way, it just redirects them to your SMTP server. If you want to redirect SMTP email you can configure this under **Networks – System – Server – SMTP Redirect.**

Copyright 2013 ValuePoint Networks, Inc. All rights reserved.

7. Starwood

The NC-3600 gateway is fully approved for Starwood's Galaxy Property Management System (PMS) for billing. The interface is bidirectional and conforms to Galaxy's Generic 2-Way HSIA Interface specification. Five bandwidth tiers are supported. Guests login with room number/lastname that is checked against the PMS database. Multiple devices can be supported on each guest registration, as required by the Starwood specifications.

In addition, we have implemented a "one step" login process that is much easier than competing gateway products, improving guest satisfaction and reducing support calls.